WHAT IS CLAIMED IS

1. A security mechanism for enabling a user to commence a session between a network peripheral device and a network, comprising:

an immutable memory element that contains first information including application software that initiates that provides security services;

a persistent memory element that contains second information to enable the security mechanism to configure the network peripheral device to different networks;

a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session; and

a tamper-evident enclosure for enclosing the memory elements.

2. The apparatus according to claim 1 wherein the security services include authentication of the security mechanism itself and authentication of the user to the network upon receipt of identification information from the security mechanism and the user, respectively.

3. The security mechanism according to claim 1 wherein the immutable memory contains a private key for encrypting the user and security mechanism identification information.

4. The security mechanism according to claim 1 wherein the immutable memory comprises a Read-Only Memory (ROM).

5. The security mechanism according to claim 4 wherein the immutable memory further includes a Write-once ROM.

6. The security mechanism according to claim 1 wherein the persistent memory comprises at least one of one of a CMOS Random Access Memory (RAM) and a Programmable Read Only Memory (PROM).

7. The security mechanism according to claim 1 wherein the volatile memory comprises a random access memory.

8. The security mechanism according to claim 1 wherein the tamper evident enclosure readily exhibits any attempt to gain access there through to the memory elements enclosed therein.

9. The security mechanism according to claim 1 wherein the physical security of the security mechanism depends on the degree of tamper resistance of the enclosure.

10. A method for facilitating a secure connection session with a user between a network peripheral device and a network, comprising the steps of:

accessing an immutable memory element that contains first information that provides security services;

accessing a persistent memory element that contains second information including configuration information to enable the security mechanism to configure the network peripheral device to the network;

accessing a volatile memory element that contains third information, including critical data for authentication; and

erasing said third information not later than the end of the connection session so no third information remains in the volatile memory between sessions.

11. The method according to claim 10 wherein the security services include authentication of the security mechanism itself and authentication of the user to the network upon receipt of identification information from the security mechanism and the user, respectively.